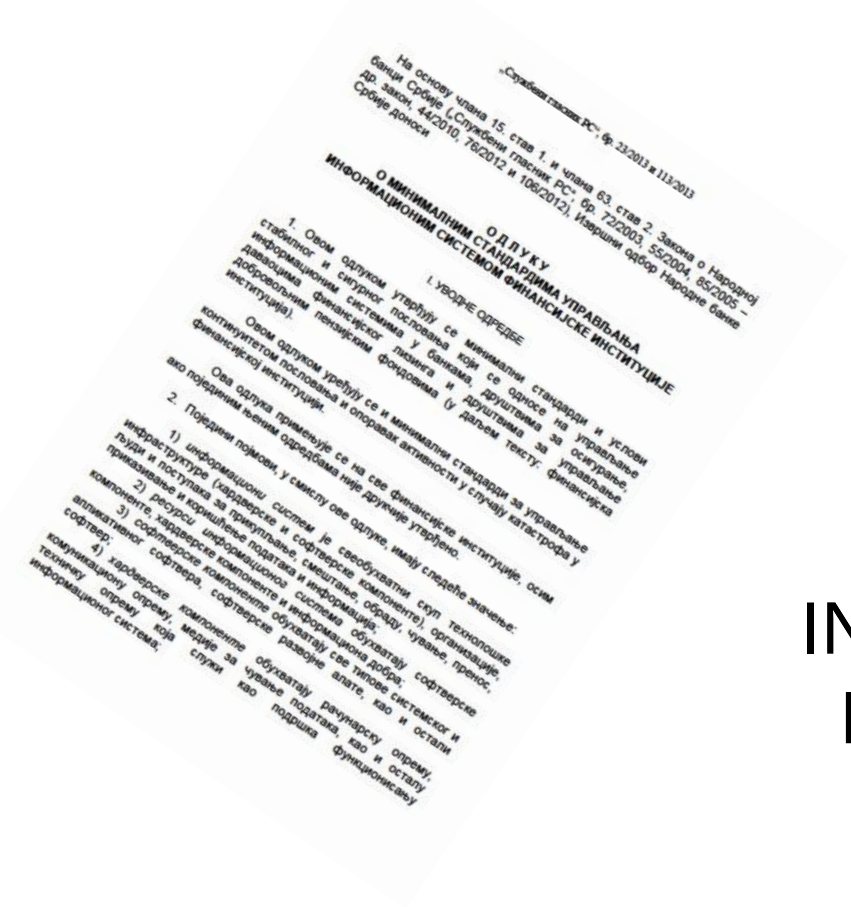


„Службени гласник РС", бр. 23/2013 и 113/2013

На основу члана 15. став 1. и члана 63. став 2. Закона о Народној банци Србије („Службени гласник РС", бр. 72/2003, 55/2004, 85/2005 – др. закон, 44/2010, 76/2012 и 106/2012), Извршни одбор Народне банке Србије доноси

ОДЛУКУ
О МИНИМАЛНИМ СТАНДАРДИМА УПРАВЉАЊА ИНФОРМАЦИОНИМ СИСТЕМОМ ФИНАНСИЈСКЕ ИНСТИТУЦИЈЕ

I. УВОДНЕ ОДРЕДБЕ

1. Овом одлуком утврђују се минимални стандарди и услови стабилног и сигурног пословања који се односе на управљање информационим системима у банкама, друштвима за осигурање, даваоцима финансијског лизинга и друштвима за управљање добровољним пензијским фондовима (у даљем тексту: финансијска институција).

Овом одлуком уређују се и минимални стандарди за управљање континуитетом пословања и опоравак активности у случају катастрофа у финансијској институцији.

Ова одлука примењује се на све финансијске институције, осим ако појединим њеним одредбама није друкчије утврђено.

2. Поједини појмови, у смислу ове одлуке, имају следеће значење:

1) информациони систем је свеобухватни скуп технолошке инфраструктуре (хардверске и софтверске компоненте), организације, људи и поступака за прикупљање, обраду, чување, пренос, приказивање и коришћење података и информација;

2) ресурси информационог система обухватају софтверске компоненте, хардверске компоненте и информациона добра;

3) софтверске компоненте обухватају све типове системског и апликативног софтвера, софтверске развојне алате, као и остали софтвер;

4) хардверске компоненте обухватају рачунарску опрему, комуникациону опрему, медије за чување података, као и осталу техничку опрему која служи као подршка функционисању информационог система.

ODLUKA O MINIMALNIM STANDARDIMA UPRAVLJANJA INFORMACIONIM SISTEMOM FINANSIJSKE INSTITUCIJE

23. Finansijska institucija je dužna da, primenom odgovarajućih kontrola, resurse informacionog sistema zaštiti od malicioznog programskog koda.

Symantec Protection Suite Enterprise Edition

Ivan Jevtić

Sales Manager

Agenda

1. Protecting the Infrastructure and Challenge
2. How Symantec Protection Suite Can Help
3. Protecting Endpoints
4. Securing Email and Web Traffic
5. Where to find more information

Infrastructure Protection Challenges

Exponential Growth of Threats

- 1000X more viruses over 3 years
- Malware Creation Kits
- 75% of malware infect less than 50 machines

Unprotected Endpoints

- Unmanaged and outdated endpoints
- Unsupported platforms

Multi-Vendor Point Products

- Inconsistent policies and reports
- Products do not share intelligence
- Licensing nightmare

Symantec Protection Suite Secures Infrastructures

Fast and Effective Protection

- Comprehensive, layered security for endpoints, messaging and web
- Complete security and recovery for desktops and laptops

Comprehensive Security

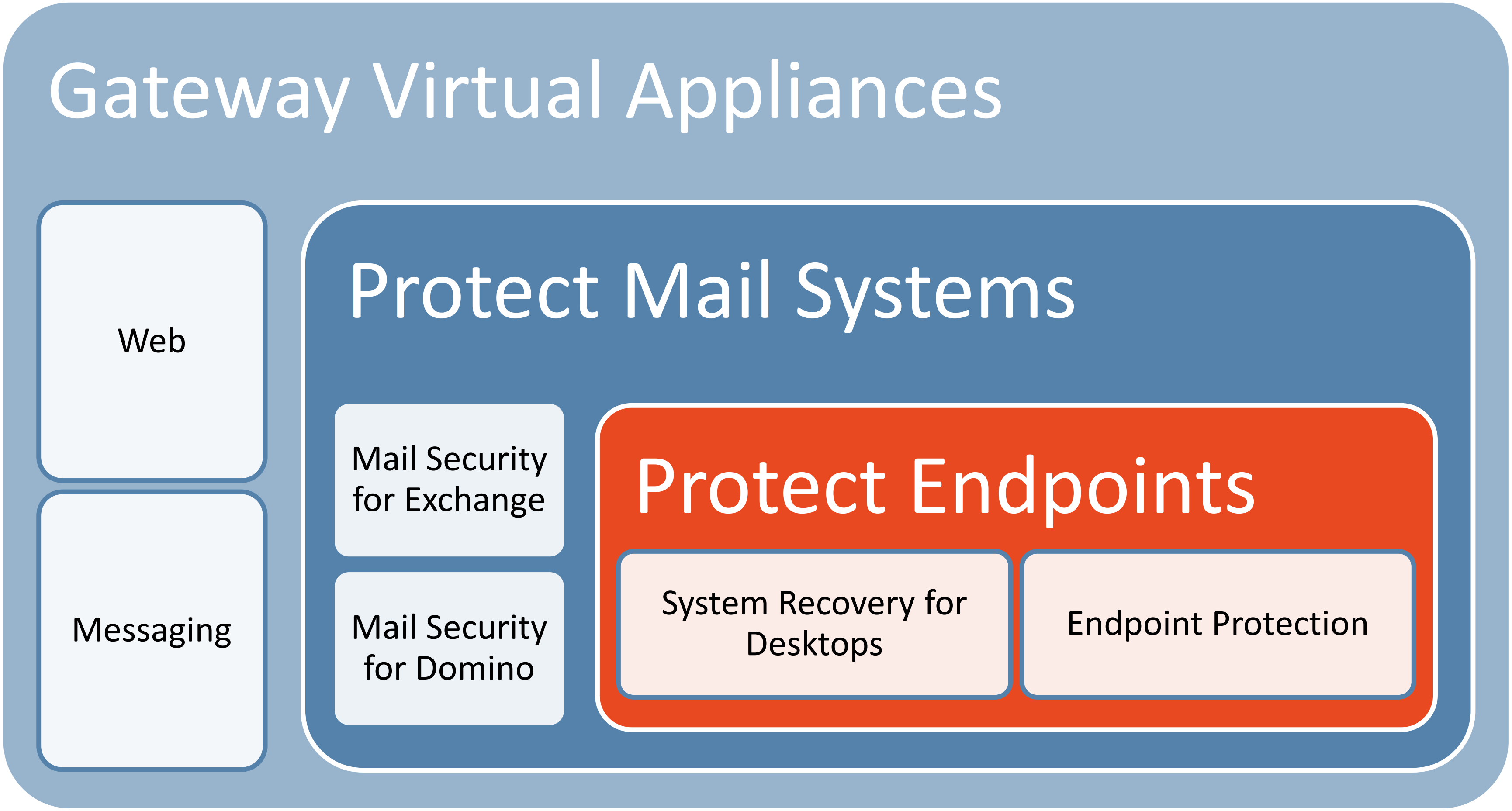
- Prevent threats from reaching endpoints
- Assume your endpoint is vulnerable
- Stops email and web based threats

Intelligent Management

- Actionable security intelligence
- Automated control
- DLP Integration
- Simplified licensing and cost savings

How is this property being protected?

Protection Suite Layers



Gateway Virtual Appliances

Web

Messaging

Protect Mail Systems

Mail Security for Exchange

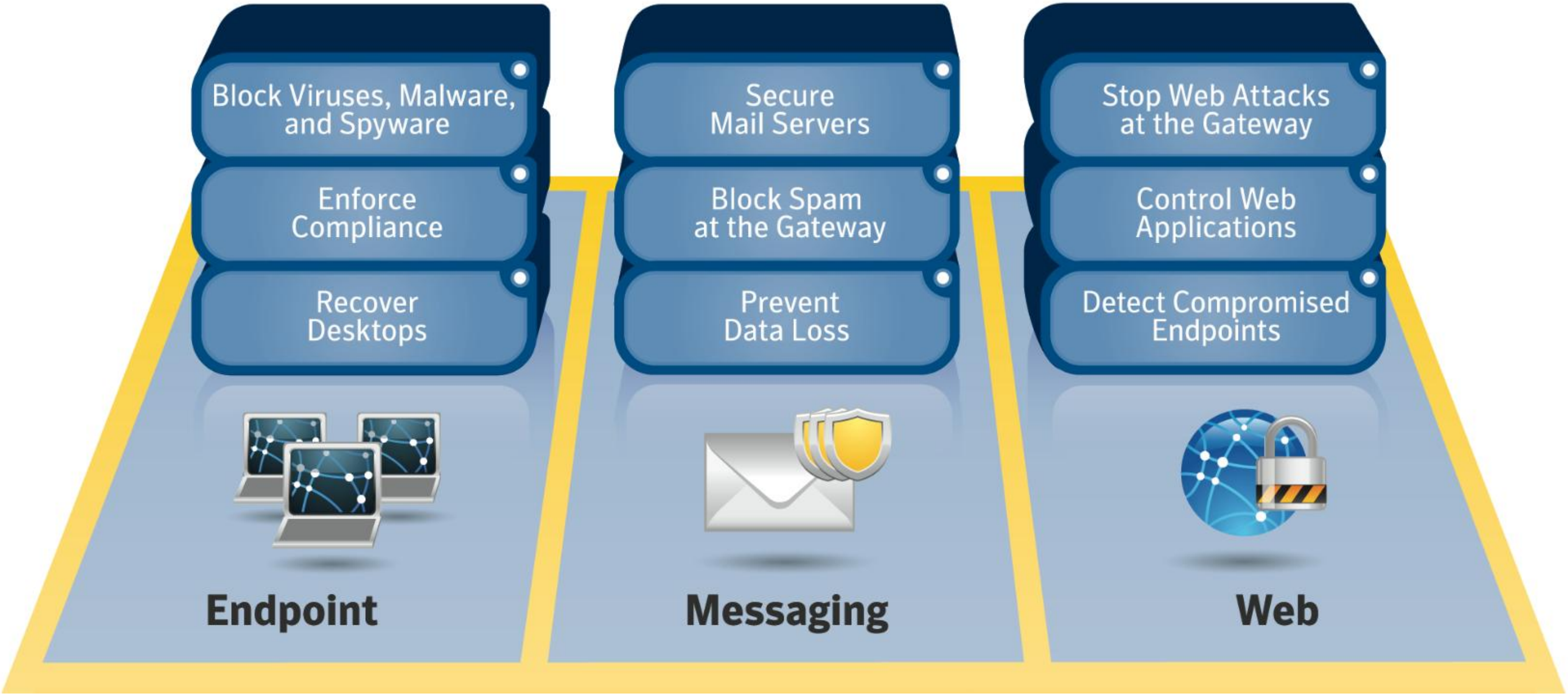
Mail Security for Domino

Protect Endpoints

System Recovery for Desktops

Endpoint Protection

Symantec™ Protection Suite Enterprise Edition



Block Viruses, Malware, and Spyware

Enforce Compliance

Recover Desktops

Endpoint

Secure Mail Servers

Block Spam at the Gateway

Prevent Data Loss

Messaging

Stop Web Attacks at the Gateway

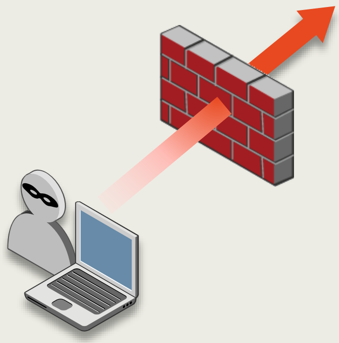
Control Web Applications

Detect Compromised Endpoints

Web

How Targeted Attacks Work

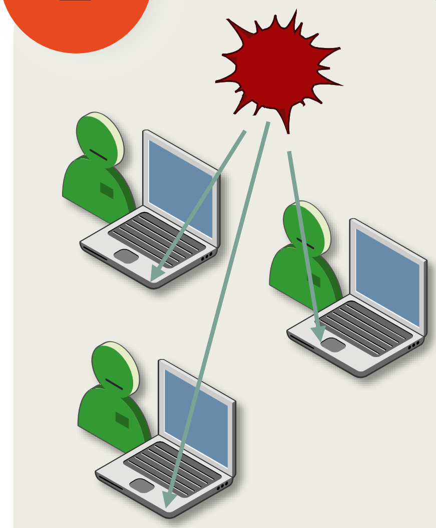
1



INCURSION

Attacker breaks into the network by delivering targeting malware to vulnerable systems and employees

2

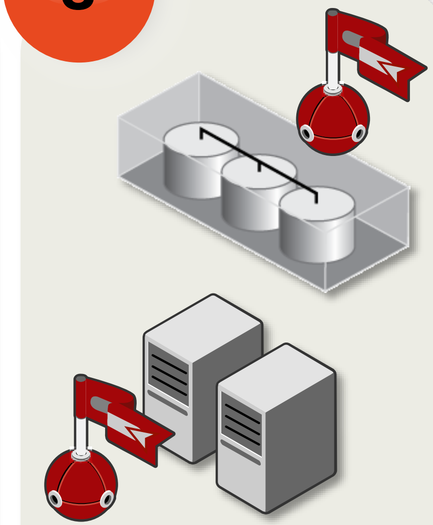


DISCOVERY

Hacker then maps organization's defenses from the inside

Creates a battle plan

3

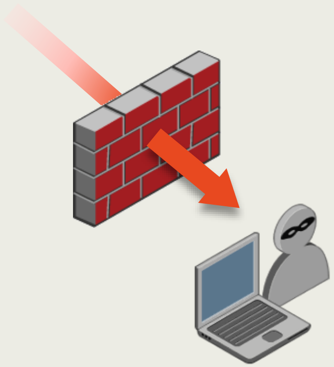


CAPTURE

Accesses data on unprotected systems

Installs malware to secretly acquire crucial data

4



EXFILTRATION

Confidential data sent to back to enemy's "home base" for exploitation and fraud

Protecting Endpoints

Comprehensive security and recovery for desktops and laptops

Symantec Endpoint Protection 12.1

Five Layers of Protection, One Solution

Firewall and intrusion prevention

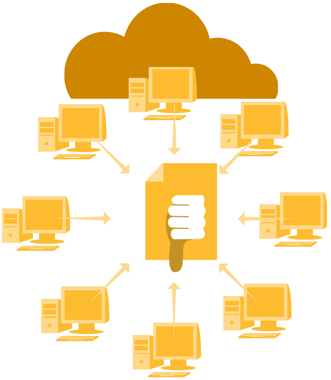
Network

Blocks malware before it spreads to your machine and controls traffic

Antivirus

File

Scans and eradicates malware that arrives on a system



Insight

Reputation

Determines safety of files and websites using the wisdom of the community

SONAR

Behaviors

Monitors and blocks programs that exhibit suspicious behaviors

Power eraser

Repair

Aggressive remediation of hard-to-remove infections

One Management Console for Both Physical and Virtual

Symantec Endpoint Protection 12

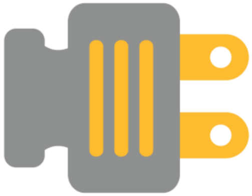
Extended Protection

System lockdown

Tightly control applications through advanced whitelisting and blacklisting

Application control

Monitor and control applications behavior



Device control

Restrict and enable access to the hardware that can be used

Host integrity

Ensures endpoints are protected and compliant

Reporting and analytics

Multi-dimensional analysis, robust graphical reporting, and an easy-to-use dashboard

(Integrated add-ons)

Symantec Insight Benefits

Turns the tables on malware authors

First approach to identify malware
not by looking at the program or its behaviors,
but by looking at who associates with it

Improves performance

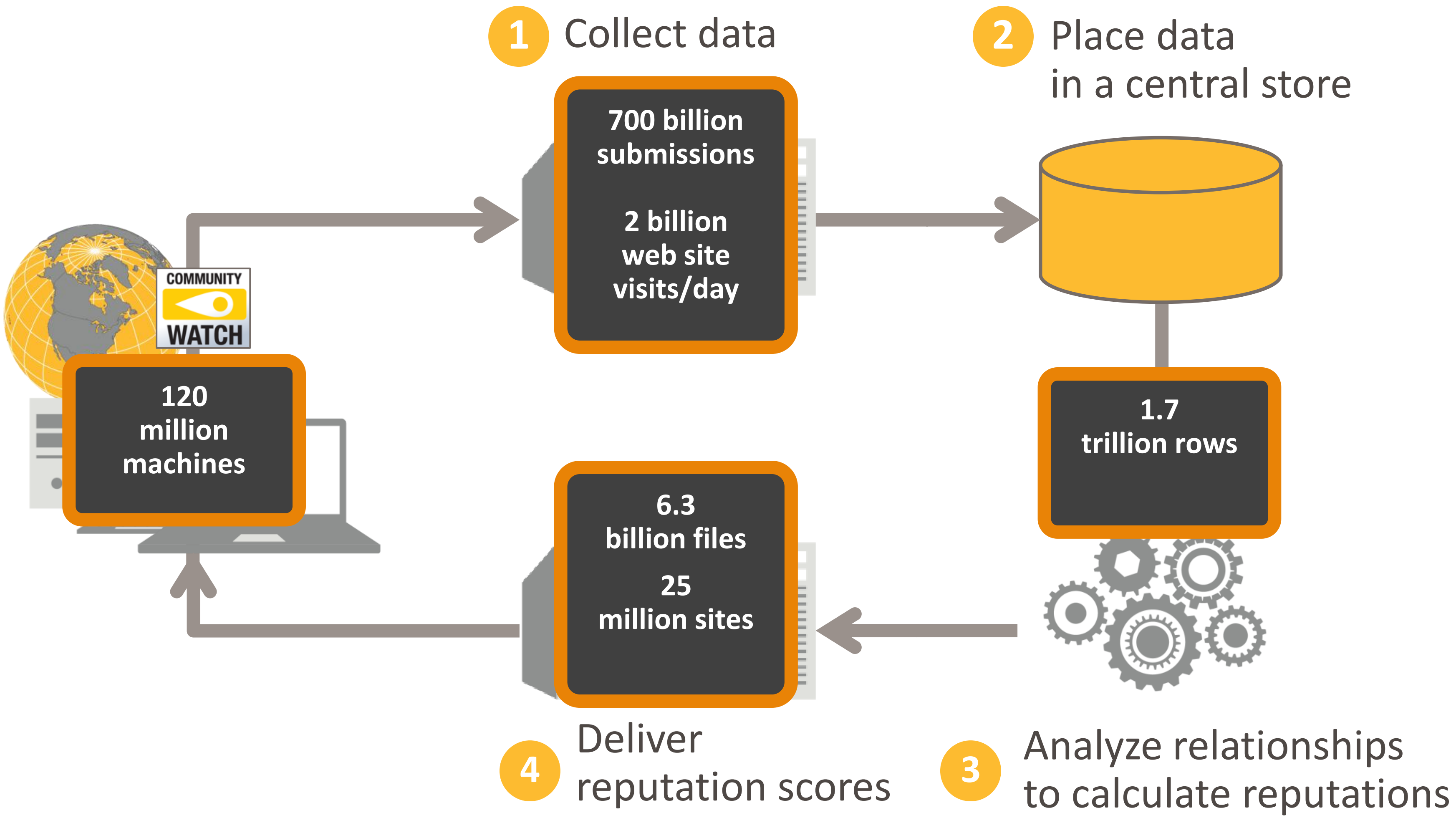
Speeds up our products by ignoring high
reputation files and focusing on the suspicious ones

Unprecedented visibility

Symantec identifies and rates
virtually every software file, good or bad, on the planet

Amplifies our other protection technologies

Symantec Insight Catches More Threats



1 Collect data

2 Place data in a central store

3 Analyze relationships to calculate reputations

4 Deliver reputation scores

120 million machines

700 billion submissions

2 billion web site visits/day

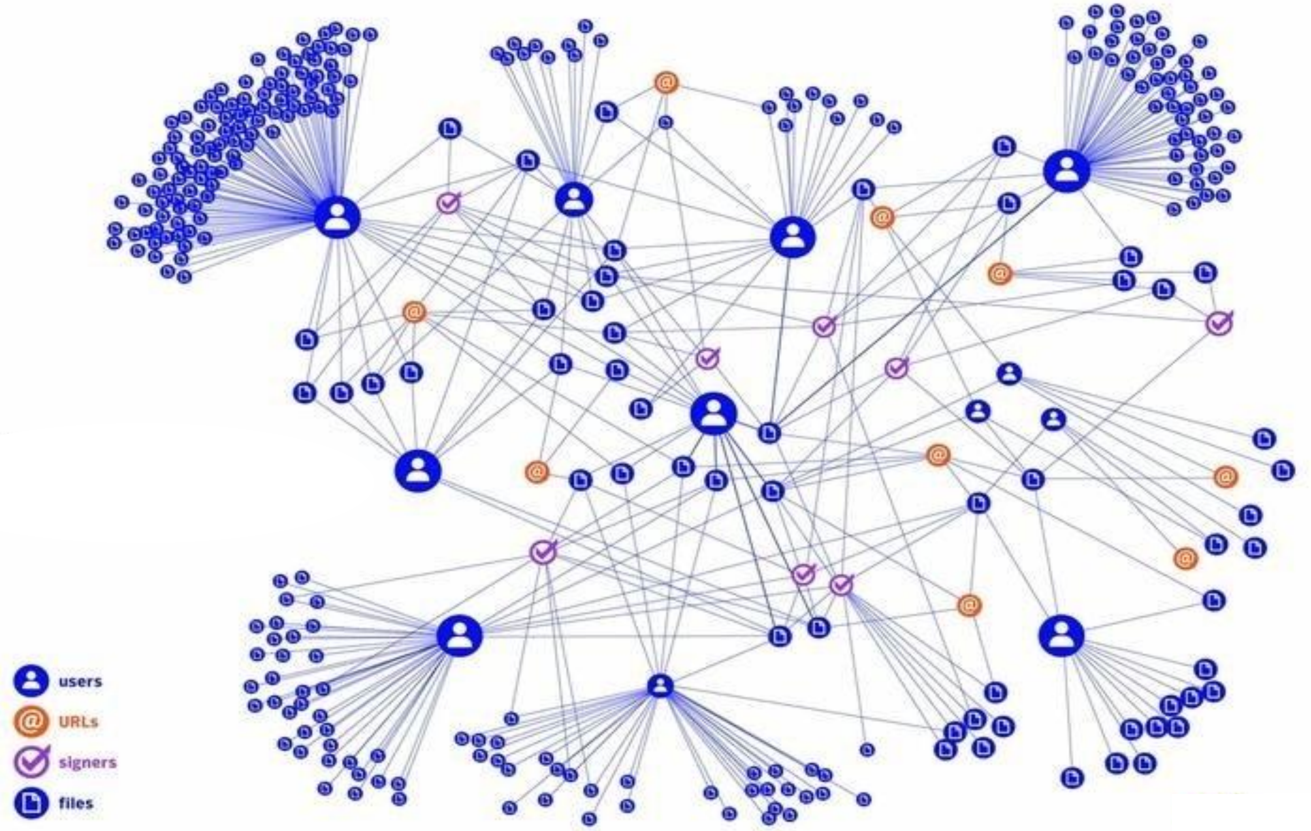
1.7 trillion rows

6.3 billion files

25 million sites

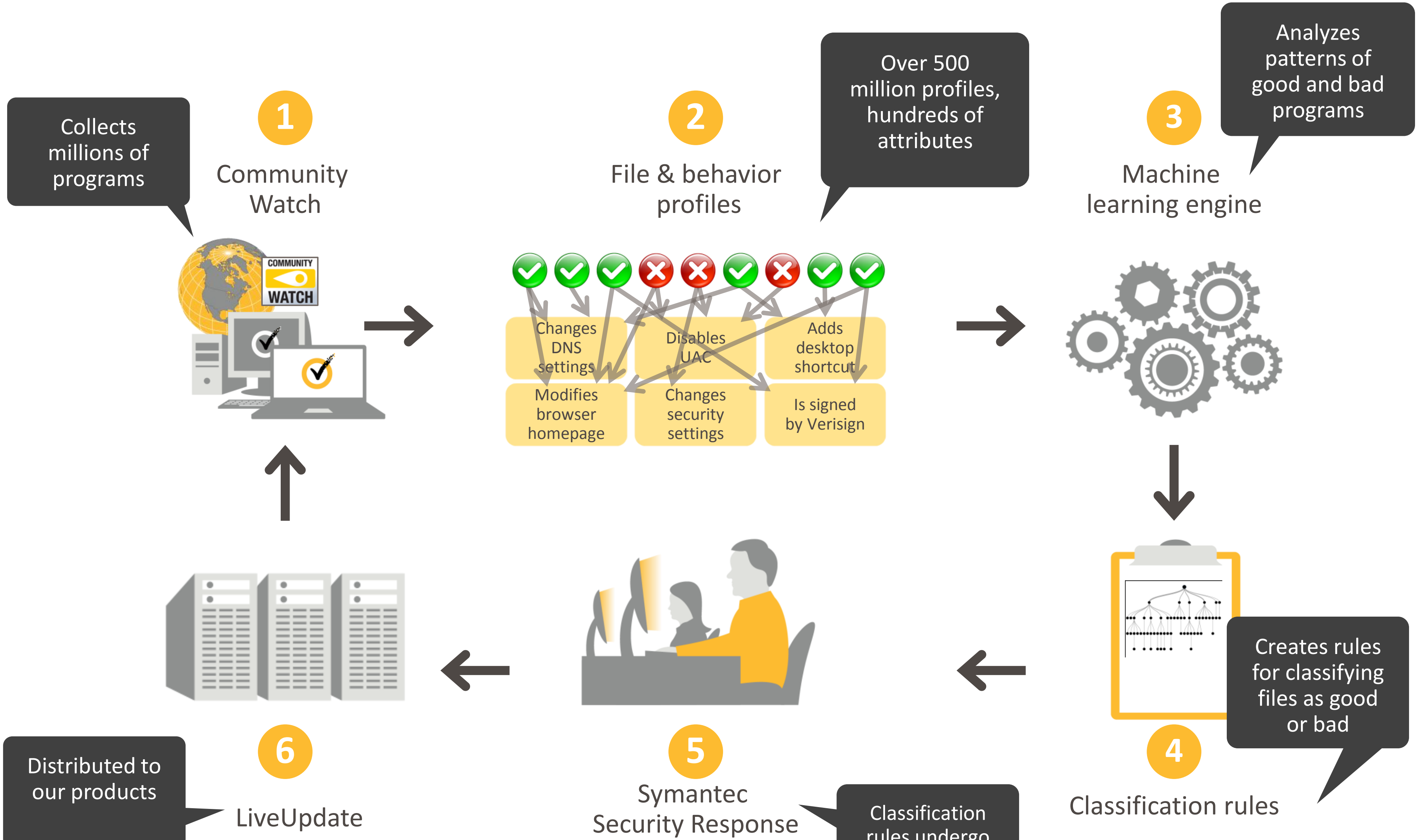
Symantec Insight Looks at Relationships

Symantec Insight makes decisions based on **who** downloads **what** from **where**…



PREDICTIVE APPLICATION

File and Behavioral Heuristics



1 Community Watch

Collects millions of programs

2 File & behavior profiles

Over 500 million profiles, hundreds of attributes

3 Machine learning engine

Analyzes patterns of good and bad programs

4 Classification rules

Creates rules for classifying files as good or bad

5 Symantec Security Response

Classification rules undergo rigorous certification

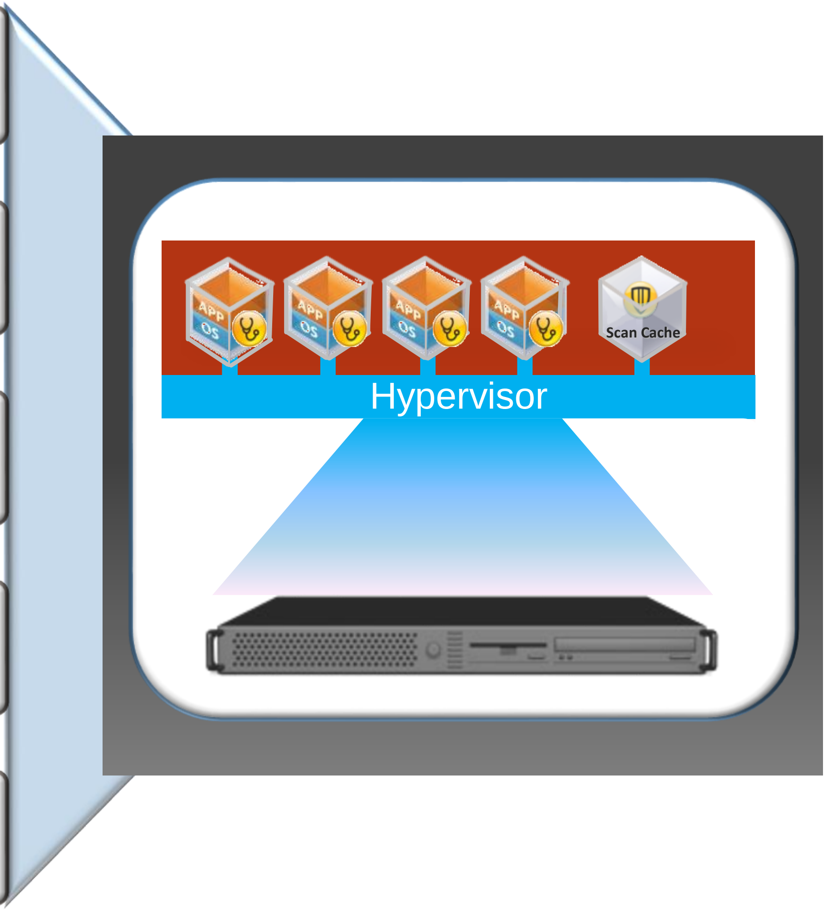
6 LiveUpdate

Distributed to our products

Virtualization Features

5 features to optimize for performance

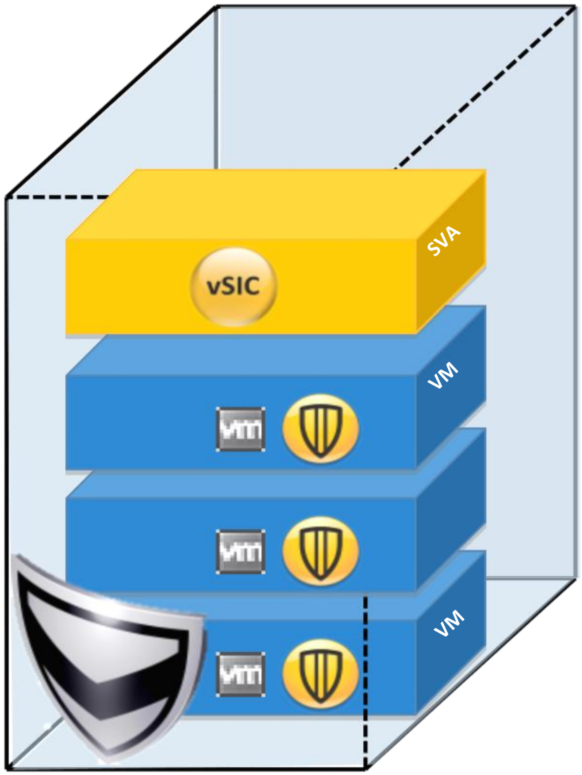
1. Virtual Client Tagging
2. Virtual Image Exception
3. Offline Image Scanner
4. Shared Insight Cache
5. Resource Leveling



vmware vShield Endpoint Integration

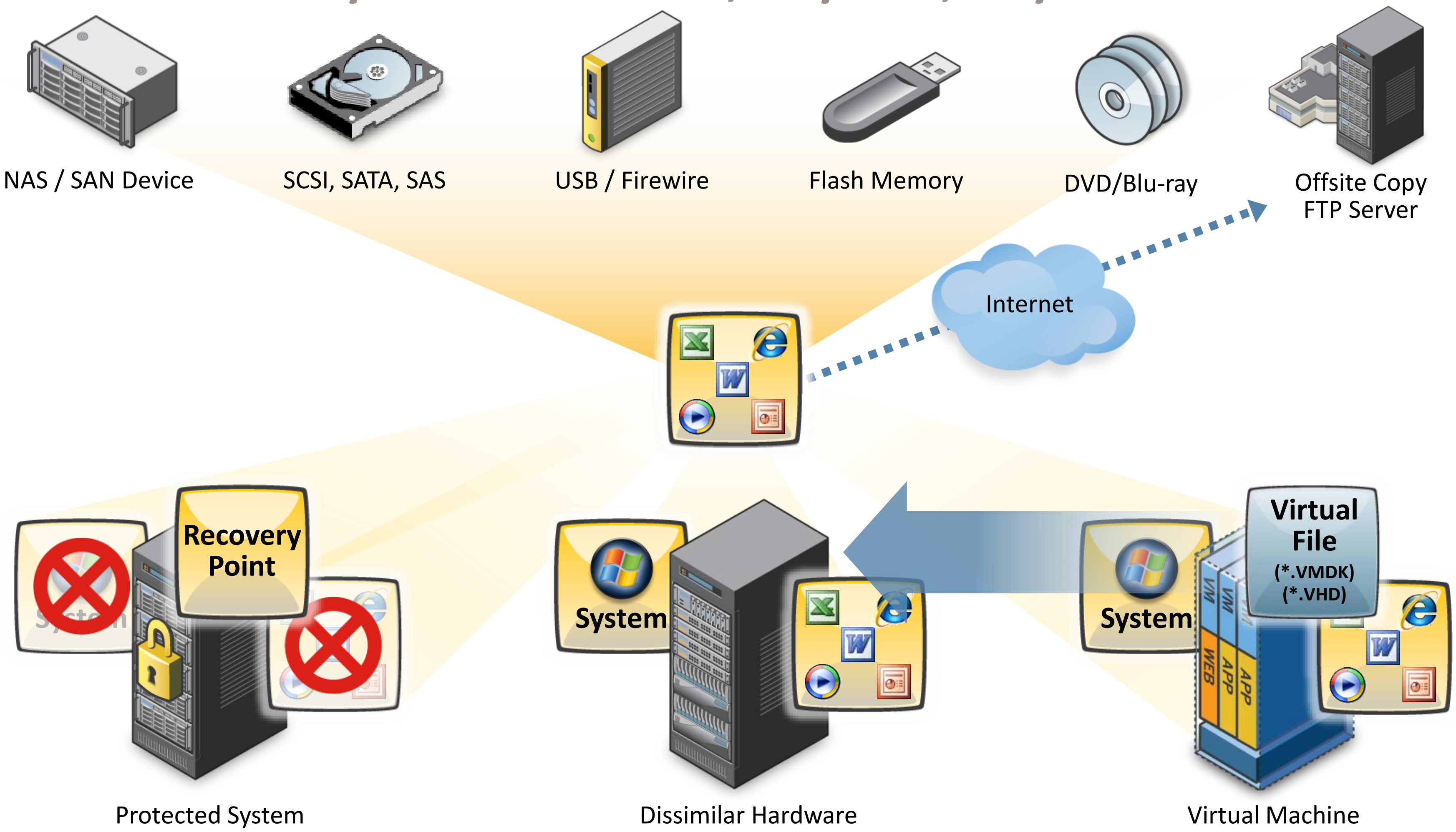
vSIC Shared Insight Cache

- Improved I/O with each scan
- De-duplicates scanning
- Prevents AV-STORM



Symantec System Recovery

Restore Your System in Minutes, Anytime, Anywhere



Messaging and Web Security

Keeping threats from reaching endpoints

Symantec Mail Security for Microsoft Exchange

Gateway Layer Protection

Inbound Threat protection

Protect Against Outdated patches and definitions

Data Loss Prevention

Email Store Scanning

Rescan Mail Store with updated definitions

Ensure clean backups

Retroactive application of policies

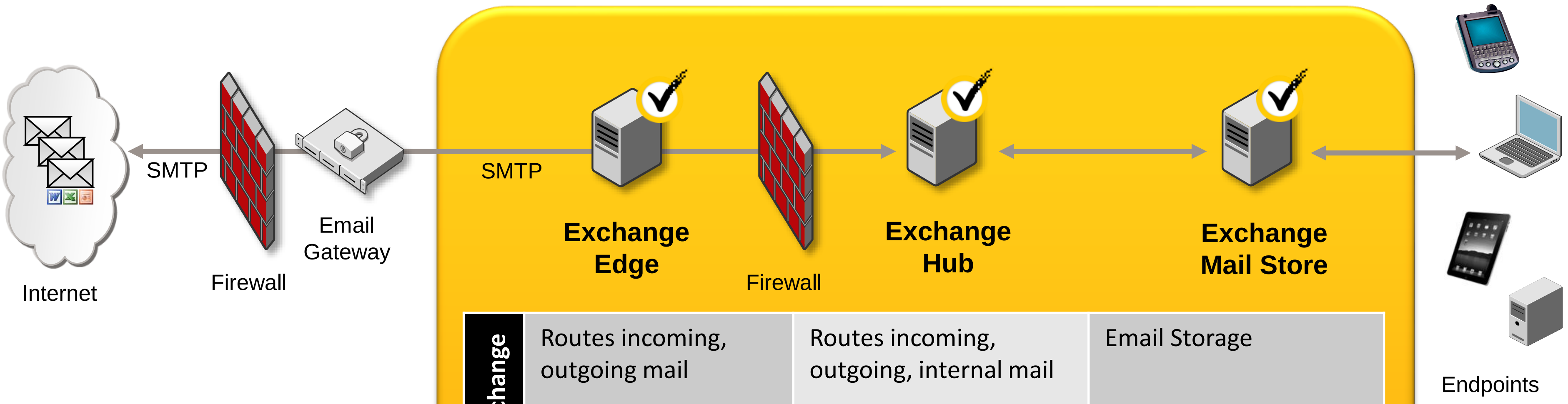
Internal Scanning

Reply-all storms

Accidental distribution of sensitive material

Internal malware

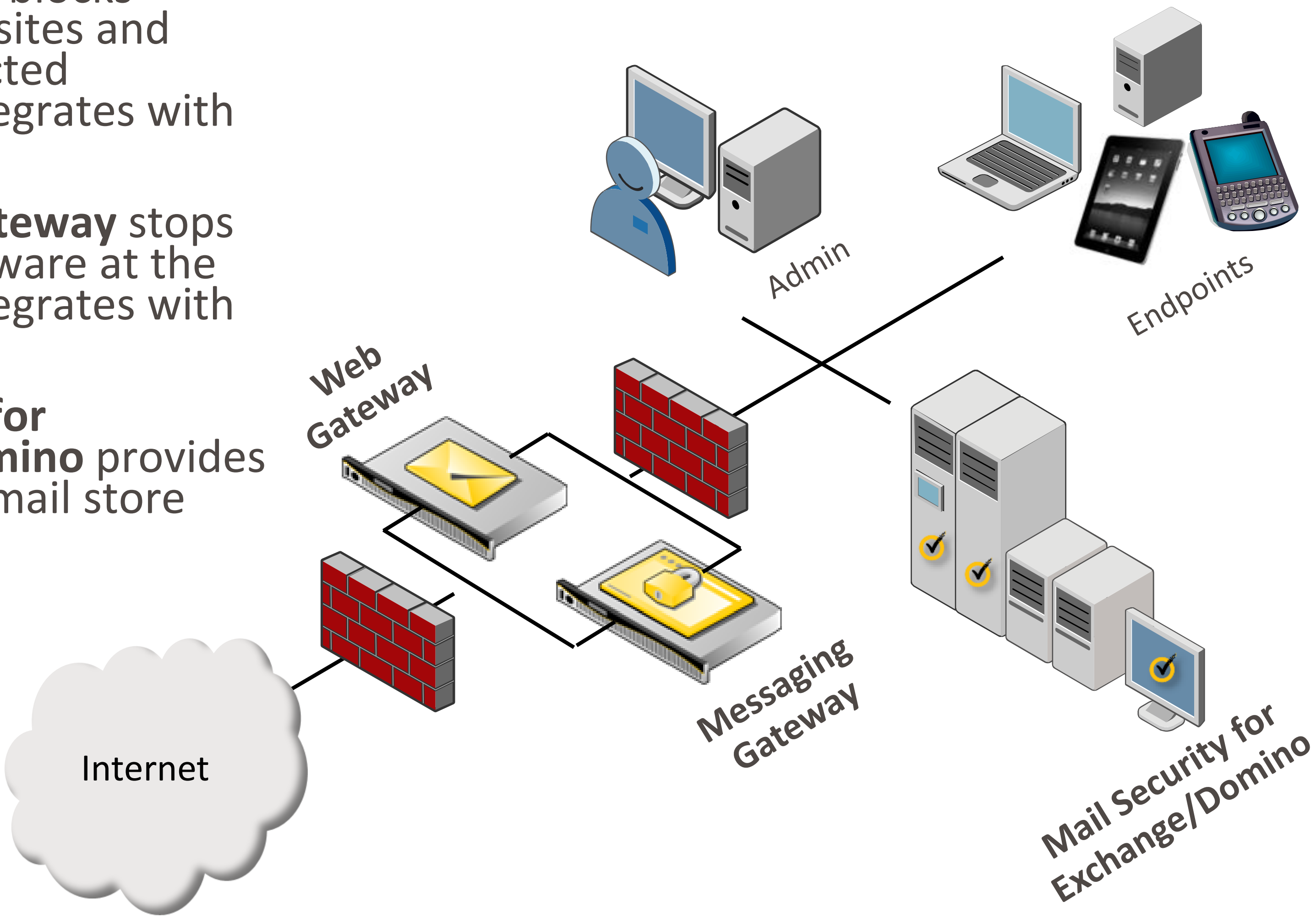
Optimized for Microsoft Exchange



Exchange	Routes incoming, outgoing mail	Routes incoming, outgoing, internal mail	Email Storage
Transport and Continuous Scanning			
Mail Security	Antivirus scanning: Edge and Hub focused; non-redundant		
	•Antispam •Reputation Services	•Antispam •Content Filtering •Attachment Blocking	•Custom Mail Store Scanning •Manual/Scheduled/ Background •Folder Selection
Global Intelligence Network			

Messaging and Web Security

- **Web Gateway** blocks malicious websites and identifies infected endpoints. Integrates with DLP.
- **Messaging Gateway** stops spam and malware at the perimeter. Integrates with DLP.
- **Mail Security for Exchange/Domino** provides internal and email store scanning



Web Gateway

Infected Client Detection

Phone Home Signature Detection

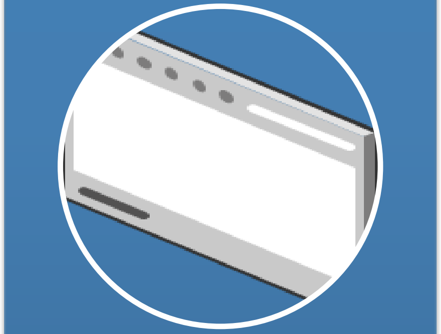
- Multi Port
- Multi Protocol

Behavioral Correlation Algorithm

- Accurately Identifies Bots on the network

Automatic Quarantine

- Limits potential damage
- Notifies end users of risk



Consolidated, Useful Reporting

- Specific Event Information
- Sort by Count, Severity, Type

Identify and prevent compromised systems from harming the organization

Adding Layers of Protection
Symantec Web Gateway

Deploying Web Gateway extends SEP protection technology at the network layer …

- Block threats *before* they reach the endpoints
- Protection for any **endpoints not configured or patched** to corporate standards
- Protection for **unmanaged or guest endpoints** on the network (up to 60% clients are unmanaged)
- Control over **network applications** (P2P, remote access etc.,)
- **Correlate** client network activity to identify **botnets**
- Symantec **Insight** protection for customers who have not upgraded to v12.1 and above

Why Symantec for Messaging Security?

Better Protection

- Award-winning anti-malware and anti-spam technologies powered by the largest threat intelligence network

Greater Control

- Market leading portfolio, including integration with DLP & Encryption

Easy Management

- Unified control and management with robust reporting on both physical and virtual appliances.

Email Control Capabilities

Integrated DLP Functionality

- Exact data matching from Symantec Data Loss Prevention (Vontu).
- Described content matching from Symantec Data Loss Prevention with over 100 pre-built dictionaries, patterns, and policy templates
- Workflow and remediation tools for incident management.
- Customizable limited rights admin access to dedicated DLP quarantine

Content Encryption

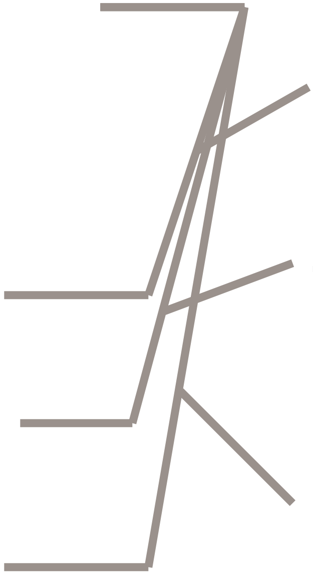
- Policy based encryption ensures the most sensitive emails are encrypted before leaving the environment
- Choice in either On-Premise encryption using PGP or hosted encryption using Symantec.cloud

Symantec DLP Integration

- Messaging Gateway integrates with Symantec DLP to protect confidential data across Endpoint, Network and Storage Systems
- Tight integration simplifies deployment and management and ensures high performance.

The Value of Symantec Protection Suite!

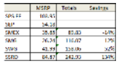
Symantec Point Products
Endpoint Protection (Mac, Linux, Win)
Mail Security for Exchange / Domino
Messaging Gateway
Web Gateway
Symantec System Recovery Desktop Edition



~12% savings from buying three licenses separately

~52% savings from buying four licenses separately

~66% savings from buying licenses five separately



	MSRP	Totals	Savings
SPS EE	102.95		
SEP	54.18		
SMEX	35.85	90.03	-14%
SMG	26.04	116.07	12%
SWG	41.99	158.06	52%
SSRD	84.87	242.93	134%

New license comparison (Band A Express) – point product vs. Protection Suite Enterprise pricing - % Savings

Thank you!

Ivan Jevtic

ivan@netpp.rs

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.